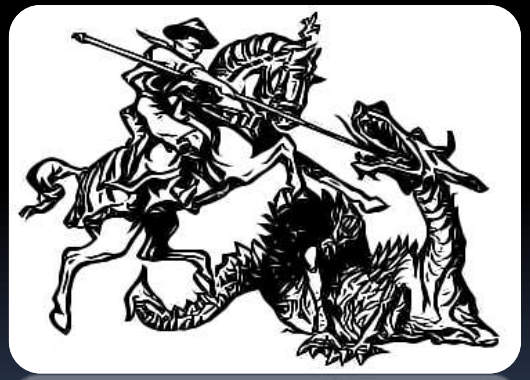
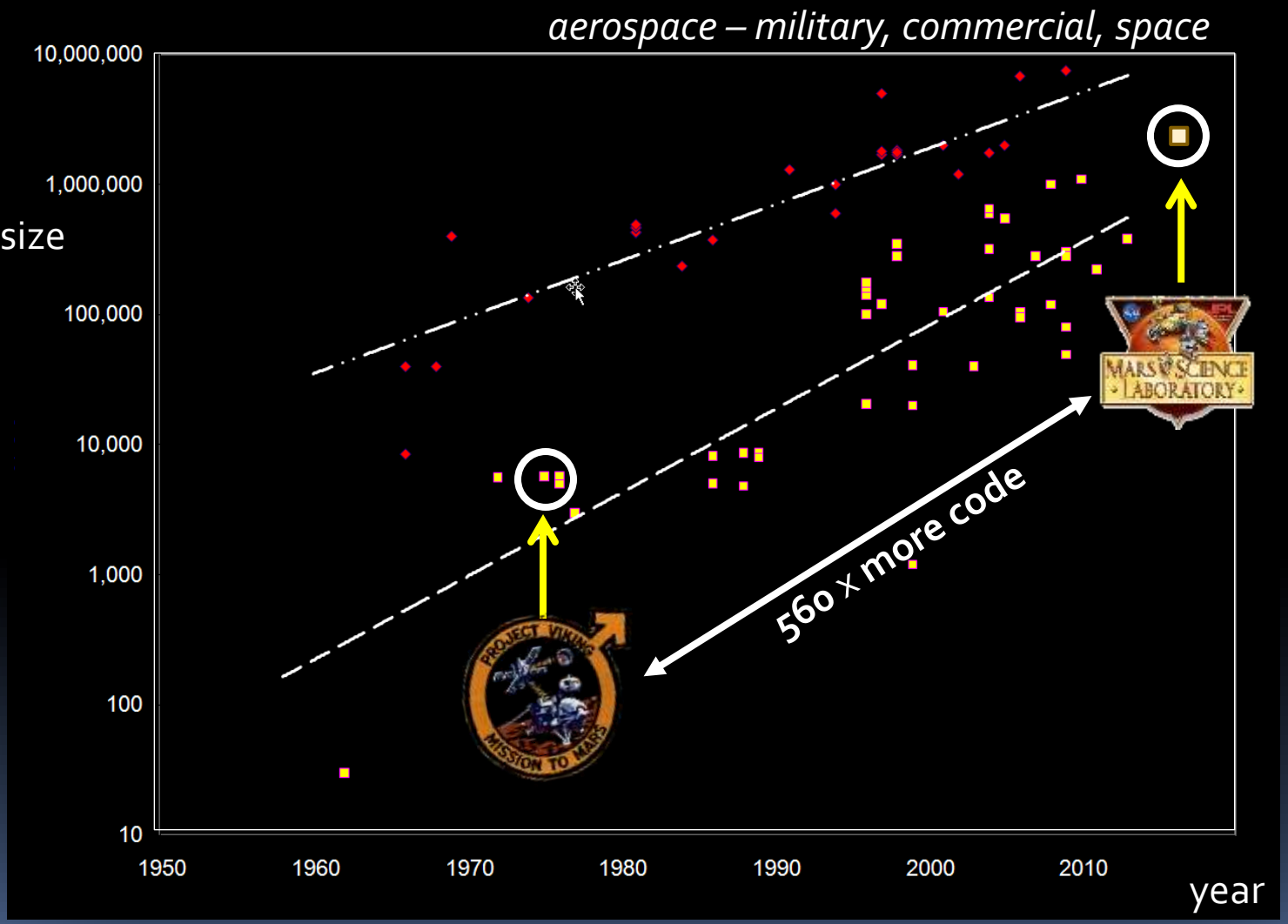
FORMAL METHODS:
PAST, PRESENT, OR FUTURE?

Gerard Holzmann
gh@jpl.nasa.gov



software verification:
a moving target



the past (~1979)
verifying concurrency


```
#define MaxSeq      5    /* window size */
#define Wrong(x)    x = (x+1) percent (MaxSeq)
#define Right(x)    x = (x+1) percent (MaxSeq + 1)
#define inc(x)      Right(x)

chan q[2] = [MaxSeq] of { byte, byte };   /* message passing channel */

active [2] proctype p5()      /* starts
{ byte NextFrame, AckExp, FrameE
  chan in, out;
  in = q[_pid];
  out = q[1-_pid];
  xr in; xs out;                  /* parti

  do
  :: nbuf < MaxSeq ->    /* outgoi
       nbuf++;
       out!NextFrame,    (FrameExp
       inc(NextFrame)

  :: q[_pid]?r,s ->          /* incor
       if
       :: r == FrameExp ->
            printf("MSC: accept pe
            inc(FrameExp)
       :: else /* ignore message *
       fi;
       do
       :: ((AckExp <= s) && (s < N
       || ((AckExp <= s) && (NextFr
       || ((s < NextFrame) && (Next
            nbuf--;
            inc(AckExp)
       :: else -> break
       od

  :: timeout -> &&     /* retransmis
       NextFrame = AckExp;
       printf("MSC: timeout\n");
       i = 1;
       do
       :: i <= nbuf ->
            out!NextFrame, (FrameE
            inc(NextFrame);
            i++
       :: else -> break
       od
  od
}
```

```
(Spin Version 6.4.4 -- 9 July 2015)
        + Partial Order Reduction

Full statespace search for:
        never claim             - (none specified)
        assertion violations    +
        cycle checks            - (disabled by -DSAFETY)
        invalid end states      +

State-vector 68 byte, depth reached 813773, errors: 0
  6048432 states, stored
  3526446 states, matched
  9574878 transitions (= stored+matched)
        0 atomic steps

Stats on memory usage (in
  647.061       memory usag


unreached in proctype p5
        tanen5:50, state 36, "-end-"
        (1 of 36 states)

pan: elapsed time 4.5 seconds
pan: rate 1,344,096 states/second
```

6 million reachable states
time to verify: < 5 seconds

the present

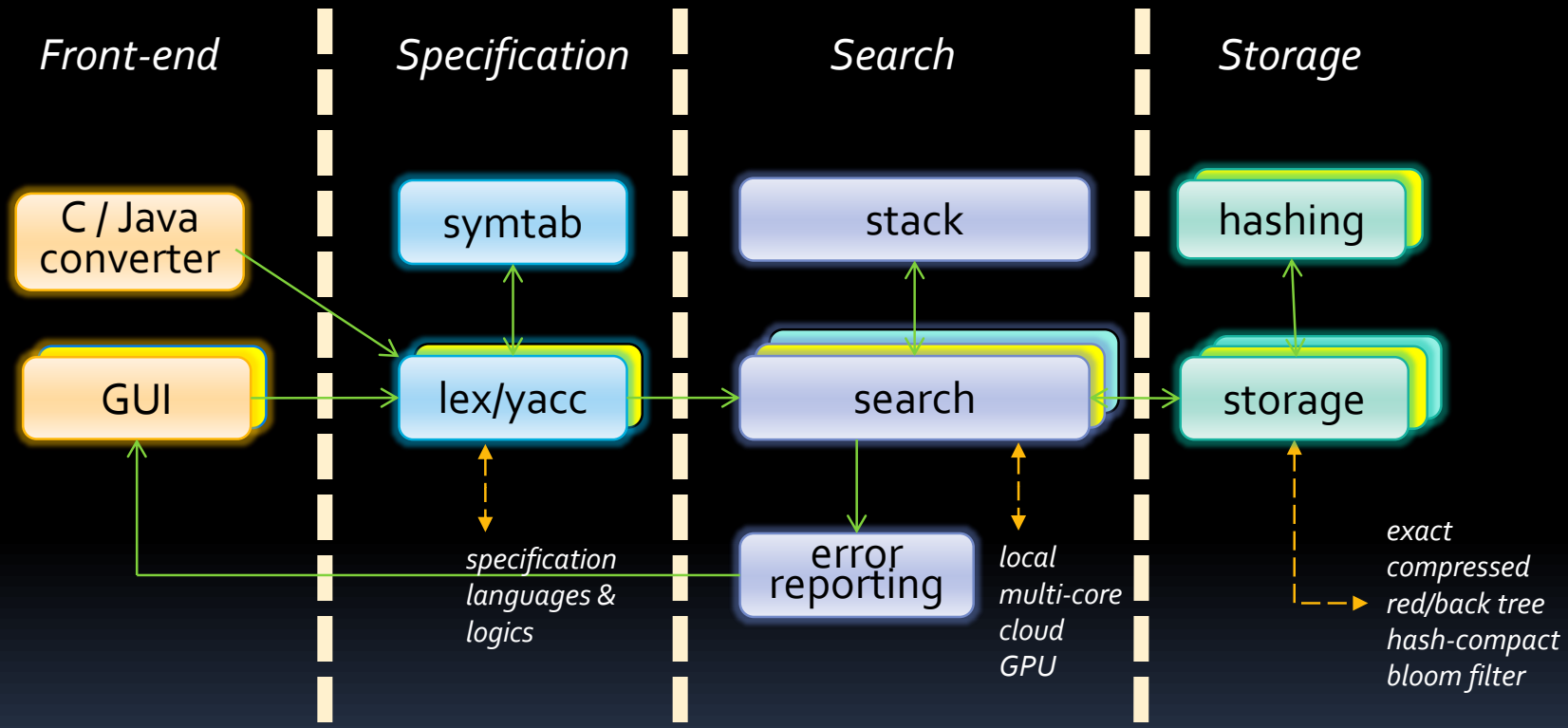
present and future

- so, today we can verify problems from 1981 just fine…
  - but what about the continuing increase in complexity?

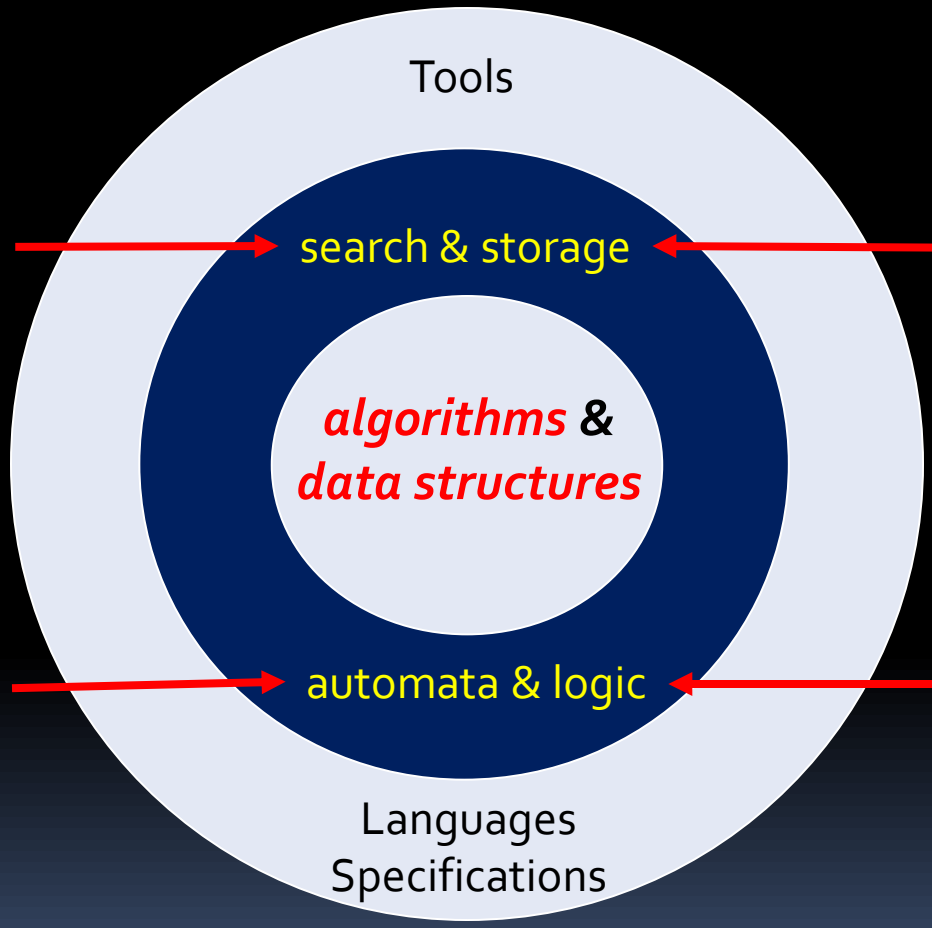
- issues that remain:
  - efficiency & scaling
    - algorithms, data structures, adaption to cloud computing

  - expressiveness & ease of use
    - logic, languages, user interfaces

how fundamental is all this?
the parts of a logic model checker



automata theoretic verification



dfs, bfs, ndfs
sequential
parallel
bounded
heuristic
randomized

local
distributed
cloud
core/disk
lossy/exact
hash functions

finite-automata
ω-automata

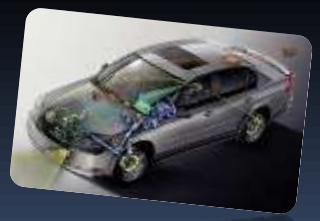
propositional &
linear temporal logic
branching time logic

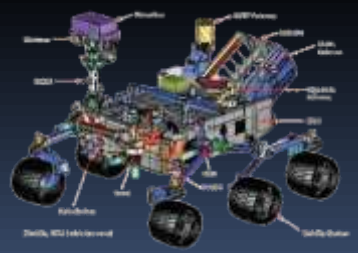
formal methods = *computer science*

(logic +
data structures +
algorithms)

+ the chance to work on some really important problems

cool!






LARS
NASA/JPL Laboratory
for Reliable Software